MCS 425 Exercise Set #4 — Spring Semester, 2008

J. Suppose that n is a randomly-chosen odd 100-digit odd integer that we wish to test for primality. We apply the Rabin-Miller test 15 times, with 15 independent random values of a. Each time the test concludes that n is a probable prime.

a) If n is actually composite, give an approximate upper bound for the probability of obtaining 15 consecutive "probable prime" outcomes from Rabin-Miller?

b) Give an approximate upper bound on the probability that n is composite?

K. The table below shows the first steps in applying the Rabin-Miller Primality Test to five integers 91, 341, 113, 209, and 131. Complete the tests by filling in each b_i that would actually be computed Rabin-Miller. **Do not fill in b_i if Rabin-Miller would not compute it.** Finally, give your conclusion: either n is ***probably prime*** or ***definitely composite***?

n	**91**	**341**	**113**	**209**	**131**
$n-1=2^s m$	$2^1 45$	$2^2 85$	$2^4 7$	$2^4 13$	$2^1 65$
a	3	2	2	2	7
$b_0 \equiv a^m \pmod n$	27	32	15	41	1
$b_1 \equiv b_0^2 \pmod n$					
$b_2 \equiv b_1^2 \pmod n$					
$b_3 \equiv b_2^2 \pmod n$					
$b_4 \equiv b_3^2 \pmod n$					
Conclusion					

L. Bob wants to send Alice a short message $M = 101$, encrypted using the RSA. Alice's public key is $(n_A, e_A) = (437,13)$.

a) What computation does Bob perform to encrypt the message. Show the steps of the computation, and give the result.

b) Alice knows than 437 factors as 19·23. How does Alice compute her private key, assuming that she chose her public key first. Compute Alice's public key using the method she would use, and give the result.

c) What computation must Alice perform to decrypt the message from Bob? Just indicate what computation Alice must perform and how many multiplications she will use in performing it; do *not* actually carry out the computation.

M. In an attempt to factor $n = 2323327$ with the quadratic sieve, using factor base $\{2,3,5,7,11,13\}$, we compute

$$\begin{array}{rcrcll}
21983^2 & \equiv & 273 & \equiv & 2^0\ 3^1\ 5^0\ 7^1\ 11^0\ 13^1 & (\text{mod } 2323327) \\
10225^2 & \equiv & 910 & \equiv & 2^1\ 3^0\ 5^1\ 7^1\ 11^0\ 13^1 & (\text{mod } 2323327) \\
4033^2 & \equiv & 1800 & \equiv & 2^3\ 3^2\ 5^2\ 7^0\ 11^0\ 13^0 & (\text{mod } 2323327) \\
30599^2 & \equiv & -1980 & \equiv & -2^2\ 3^2\ 5^1\ 7^0\ 11^1\ 13^0 & (\text{mod } 2323327) \\
22965^2 & \equiv & -4004 & \equiv & -2^2\ 3^0\ 5^0\ 7^1\ 11^1\ 13^1 & (\text{mod } 2323327) \\
15089^2 & \equiv & -8125 & \equiv & -2^0\ 3^0\ 5^4\ 7^0\ 11^0\ 13^1 & (\text{mod } 2323327) \\
27563^2 & \equiv & -8960 & \equiv & -2^8\ 3^0\ 5^1\ 7^1\ 11^0\ 13^0 & (\text{mod } 2323327) \\
18730^2 & \equiv & -9477 & \equiv & -2^0\ 3^6\ 5^0\ 7^0\ 11^0\ 13^1 & (\text{mod } 2323327)
\end{array}$$

Use the information above to find a nontrivial factorization of 2323327.

Hint: Find two rows above such that, when the rows are multiplied together, each of 2, 3, 4, 7, 11, and 13 have even exponents. Note either both rows, or neither, must have a minus sign. In general, any subset of the rows you choose must contain an even number of rows with minus signs.

N. Bob's public and private ElGamal keys are $(p_B, \alpha_B, \beta_B) = (59, 6, 55)$ and $a_B = 37$. Bob receives the ElGamal encrypted message (50, 30) from Alice. How does he decrypt the message, and what does he obtain?